IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAR 4 2019

UNITED STATES OF AMERICA

v.

BARRENCE MARK ANTHONY

Case No. 1:19-MJ-117

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Jamie DeCastro, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Computer Crime Investigative Unit (CCIU) of the U.S. Army Criminal Investigation Command ("USACIDC"), and have been employed in that position since December 2016. Previously, for approximately five years, I served as an Information Assurance Analyst with U.S. Army Cyber Command, Fort Belvoir, VA. In addition to my training as a criminal investigator, I am trained in computer incident response, digital evidence acquisition, and computer forensics. I received training from the Department of Defense Cyber Investigations Training and the Federal Law Enforcement Training Center, and hold a Master's Degree in Information Systems Management from Keller Graduate School of Management of DeVry University.

2. As a Special Agent of USACIDC, I am authorized to investigate crimes involving violations of the Uniform Code of Military Justice, and other applicable federal laws, where there is an Army interest, including 18 U.S.C. § 1030 (Computer Fraud and Abuse Act).

3. The facts in this Affidavit come from my own personal observations, my training and experience, and information obtained from other agents and witnesses. Because this Affidavit is for the limited purpose of establishing probable cause for a criminal complaint, it does not set forth every fact learned in the course of this investigation by me or known to the government.

4. I make this Affidavit in support of an application for a criminal complaint and arrest warrant in an investigation involving **BARRENCE MARK ANTHONY**. As set forth herein, probable cause exists to believe **ANTHONY** has violated 18 U.S.C. § 1030(a)(2)(C), which criminalizes intentionally accessing a computer without authorization and obtaining information from a protected computer that exceeds $5,000 and that was committed in furtherance of any criminal act in violation of the laws of any state.

SUMMARY OF PROBABLE CAUSE

5. On or about January 25, 2016, **ANTHONY** became a Systems Engineer with VICTIM COMPANY. VICTIM COMPANY is located in Arlington, Virginia in the Crystal City neighborhood, which is in the Eastern District of Virginia. ANTHONY worked for VICTIM COMPANY in its Crystal City offices. VICTIM COMPANY provides information technology (IT) engineering services to its customers. On September 29, 2015, VICTIM COMPANY was awarded a government contract to provide technology services for the maintenance and customization of the U.S Army's Office of the Chief of Chaplains' (OCCH) Army Chaplain Corps Religious Support System (CCRSS), which remains operational today. VICTIM COMPANY was contracted to provide these services by building and managing the Financial Management System (FMS) SharePoint application, hosted on Amazon Web Services (AWS). As part of its contract, VICTIM COMPANY also provided a support service desk for the Army's CCRSS users. VICTIM COMPANY is the only authorized and contracted company for operation of the Army Chaplain

Corps' system that resides on the AWS cloud-based infrastructure. Approximately 9,000 users across the world access the CCRSS, providing a business application for Army Chaplains to conduct their ministries. The SharePoint application tracks financial transactions resulting from Army fund distributions in the form of grants and contributions received from church affiliated gatherings.

6. As part of his responsibilities as a Systems Engineer, **ANTHONY** had access to network systems and passwords for the U.S. Army's Amazon Web Services cloud infrastructure, which housed servers, operating systems, authentication systems, cyber security monitoring systems, routing networks, and application services for the Army Chief of Chaplains' Office in the Pentagon.

7. The investigation began after a computer user, later identified as **ANTHONY**, accessed U.S Army's Office of the Chief of Chaplains' (OCCH) Army Chaplain Corps Religious Support System (CCRSS) network without authorization numerous times between in and around December 2016. This activity began on or about December 7, 2016 -- the day before **ANTHONY**'s termination from VICTIM COMPANY – and continued after his termination.

8. As explained below, the investigation revealed that in December 2016, **ANTHONY** accessed U.S Army's Office of the Chief of Chaplains' (OCCH) Army Chaplain Corps Religious Support System (CCRSS) servers and stole eight machine images by hosting them on his own personal Amazon Web Services account and disrupted a critical website rendering it unavailable during a training course.

PROBABLE CAUSE

9. On or about January 25, 2016, **ANTHONY** began working at VICTIM COMPANY as a Systems Engineer. As part of his responsibilities as a Systems Engineer, **ANTHONY** had access

to network systems and passwords for the U.S. Army's Amazon Web Services cloud infrastructure, which housed servers, operating systems, authentication systems, cyber security monitoring systems, routing networks, and application services for the Army Chief of Chaplains Office in the Pentagon. The name of the overall System is the Chaplain Corps Religious Support System (CCRSS), which remains operational today.

10. Normally, multiple VICTIM COMPANY employees have access to the master password for an encrypted file containing all other CCRSS passwords, but on December 7, 2016, **ANTHONY** was the only person with access to that master password. VICTIM COMPANY's computer logs show that on that same day, December 7, 2016, all user and administrator accounts except **ANTHONY**'s were deleted from the CCRSS application. This action had the impact of leaving **ANTHONY** with sole control of the AWS system and locking out all other authorized users.

11. Later on December 7, 2016, VICTIM COMPANY personnel then tried to retrieve access to the master password for the encrypted file containing all the other CCRSS passwords by contacting **ANTHONY**, but **ANTHONY** refused to provide access to the file at that time.

12. VICTIM COMPANY provided me with copies of emails from domain name registrar GoDaddy Inc. to **BARRENCE ANTHONY**, dated December 7, 2016 and December 8, 2016. The correspondence included a request from GoDaddy to **ANTHONY** to verify a requested change of the registrant for the chaplaincorps.net domain name from "VICTIM COMPANY" to "Anthony Enterprises." A request of this nature is only prompted once the requestor initiates a change to the account. Though **ANTHONY** was not authorized to make this change, the registrant was, nonetheless, changed. VICTIM COMPANY's Incident Response Team, which looked into

the matter, found that "Anthony Enterprises" had the mailing address for his residence and the email address barrence_anthony@yahoo.com.

13. Moreover, on the morning of December 8, 2016, 19 files belonging to VICTIM COMPANY were deleted. Computer log files reveal that "Barrence Anthony" deleted the files. Two additional files were downloaded from VICTIM COMPANY's project folder which contained the crucial CCRSS AWS service account information and network diagram files.

14. Later on December 8, 2016, at approximately 1:30 p.m. EST, VICTIM COMPANY formally terminated **ANTHONY**. **ANTHONY** was told by VICTIM COMPANY via email to "[please desist use of the VICTIM COMPANY email account henceforth...I remind you that at your departure, you declined from performing the transition of account information and passwords I requested from you. Because this information is U.S. Government information under VICTIM COMPANY's custodianship, I recommend that you provide this information immediately to avoid potentially serious legal infractions... **Effective as of our conversation today at 1:30pm, please note that any attempt to login to the CCRSS systems or AWS architecture is unauthorized access.** As with the U.S Government information mentioned earlier herein, I remind you these are federal government systems and unauthorized use or access may constitute serious legal infractions. Thanks in advance for your prompt cooperation." The emphasis in this paragraph is your affiant's.

15. Records obtained from VICTIM COMPANY show **ANTHONY** continued to disrupt U.S Army's Office of the Chief of Chaplains' (OCCH) Army Chaplain Corps Religious Support System (CCRSS) computer network systems on December 8, 2016 after he was terminated and notified that any additional activity on the U.S Army's Office of the Chief of Chaplains' (OCCH) Army Chaplain Corps Religious Support System (CCRSS) network would be unauthorized access.

On or about the evening of December 8, 2016, the defendant BARRENCE ANTHONY made sixteen backup images of the U.S. Army's CCRSS web application, which included the intellectual property of the servers and all servers and web applications. The backup images, known as Amazon Machine Images or AMIs, were then shared, without authorization from VICTIM COMPANY, with Amazon Web Services account #779908447613. An AMI is a duplicate of a server instantiation and its hosted applications that provides the information required to recreate the U.S. Army Chaplain Corps' enterprise, applications and the CCRSS. Amazon Inc. provided information showing that AWS account #779908447613 belonged to the defendant **BARRENCE ANTHONY** and that the registration address for that account corresponded to the defendant **BARRANCE ANTHONY's** residential address.

16. The VICTIM COMPANY has revealed that the information on the AMI's that **ANTHONY** shared with his AWS accounts is valued at $1,136,548.82. In addition, **ANTHONY's** unauthorized taking of the AMI's without authorization constituted Grand Larceny in violation of Virginia Code Ann. § 18.2-95.

17. Moreover, log files provided by VICTIM COMPANY show that on or about 8:53 p.m. (EST) on December 8, 2016, after **ANTHONY** was terminated, but while he possessed the sole administrator account on the system, a "Sysprep" command against a test server named CARSSTS02 that was part of the U.S. Army CCRSS Web Application system on the AWS cloud-based infrastructure was executed. A Sysprep command wipes out all information on a particular server. That is what happened here. Since there were not any backups of the CARSSTS02 test server, all information on this server was lost, causing VICTIM COMPANY engineers to have to rebuild another test server. Because **ANTHONY** had sole administrative access, there is probable cause to believe that he initiated the Sysprep command.

18. While VICTIM COMPANY was able to regain access to its systems by December 11, 2016, there is probable cause to believe that **ANTHONY** continued to disrupt U.S Army's Office of the Chief of Chaplains' (OCCH) Army Chaplain Corps Religious Support System (CCRSS) networks. For example, server logs provided by VICTIM COMPANY revealed that from approximately December 11, 2016 through December 22, 2016, the U.S. Army CCRSS Web Application system hosted on the AWS cloud-based infrastructure sustained 37,439 brute force cyber-attacks, causing the system to be inaccessible. This was due to attacks from multiple accounts, three of which include: "BarrenceAnthony," "Ba rrence Anthony" and "CHAPLAINCORPSXbanlhony" The brute force attacks necessitated a shutdown of a server that provides access to the Army's CCRSS enterprise for System Administrators, as well as being an email relay for users in the Chaplain community; this server was off-line for more than two weeks as a result of the attack.

19. Additionally, computer logs also showed a login to the SharePoint application and the CARSSSTS02.chaplaincorps.net server after **ANTHONY** was terminated. Furthermore, as a result of **ANTHONY**'s continued interference with U.S Army's Office of the Chief of Chaplains' (OCCH) Army Chaplain Corps Religious Support System (CCRSS) systems, a critical website was unavailable during a training course. On December 12, 2016, the Chaplain Center & School was scheduled to provide the Chaplaincy Resource Management course (part of the OCCH-CCRSS, managed by VICTIM COMPANY) to 19 students at Fort Jackson, SC. However, the website used for the course was unavailable that morning. Approximately seven hours of training time was lost due to the outage.

INTERVIEW WITH BARRENCE ANTHONY

20. On September 18, 2018 **ANTHONY** was interviewed in a non-custodial setting. **ANTHONY** participated in a visual and audio statement, where he admitted to deleting files from the U.S. Army Chaplain Corps SharePoint site and controlling access into the VICTIM COMPANY Amazon Web Services account that hosts servers for the U.S. Army Chaplain Corps mission. He also admitted cross-account sharing those Amazon Machine Images from VICTIM COMPANY's account with his personal Amazon Web Services account registered to Anthony Enterprises. Additionally, **ANTHONY** admitted to converting VICTIM COMPANY's account information to his own, and admitted his motivations for the disruption and damage to VICTIM COMPANY were his efforts to punish the company for his termination.

CONCLUSION

Based on the foregoing, I believe that there is probable cause to support the attached complaint charging **BARRENCE ANTHONY** with a violation of Title 18, United States Code, Section 1030(a)(2)(C) and the associated arrest warrant.

JAMIE DECASTRO, Special Agent
U.S. Army Criminal Investigation Command

Subscribed and sworn to before me on March 4, 2019.

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

Honorable Theresa C. Buchanan
United States Magistrate Judge
Alexandria, Virginia